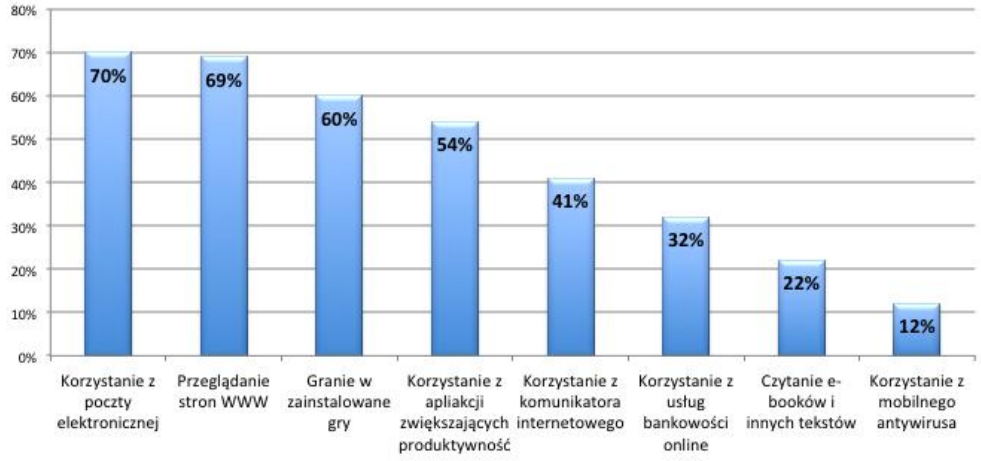
Dawid Pikuła[57]

(Nie)bezpieczne urządzenia mobilne

WSTĘP

Początek drugiej dekady XXI charakteryzuje się dynamicznym wzrostem liczby urządzeń mobilnych (Punzalan, 2012) – tak zwanych smartfonów. Według badań IDC trend ten będzie stale kontynuowany, by w roku 2017 smartfony stanowiły blisko 70% wszystkich telefonów komórkowych (Thomson, 2013).

Użytkowanie smartfona przynosi wiele korzyści (Cassavoy, 2011). Posiadacz smartfona nie musi spędzać czasu przed monitorem komputera w oczekiwaniu na ważną wiadomość e-mail. Może wyłączyć komputer, będąc przy tym cały czas obywatelem społeczności internautów. Po nadejściu wiadomości zostanie o tym fakcie poinformowany i będzie mógł od razu na nią odpisać. Innym przykładem ekspansji funkcjonalności znanych z tradycyjnych komputerów na smartfony jest przejęcie roli magazynu dokumentów elektronicznych, zdjęć, filmów czy muzyki, a nawet roli osobistego organizera. Zestawienie najczęściej wykorzystywanych funkcji oferowanych przez najnowsze smartfony przedstawiono na rysunku 1.



Rys. 1 Najczęściej wykorzystywane funkcje smartfonu (Źródło: Kaspersky Lab, 2011)

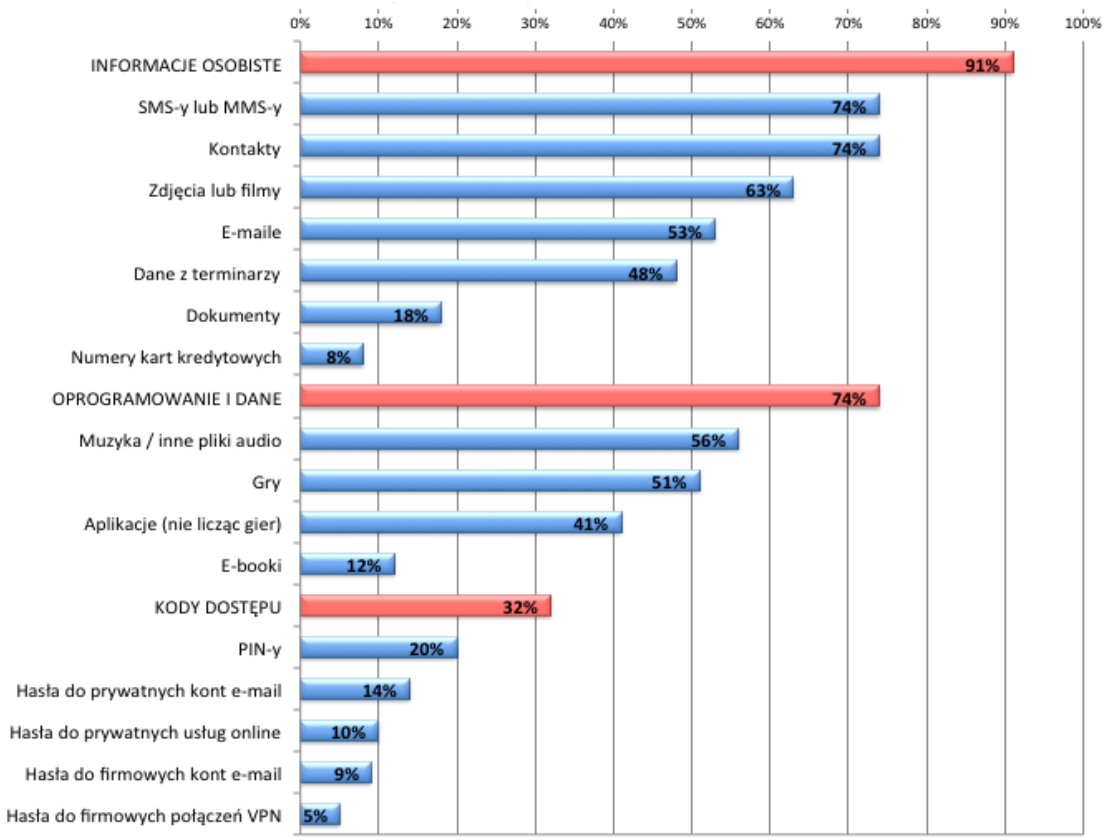
Smartfony są coraz częściej wykorzystywane także w biznesie. Dzięki takiej uniwersalności stały się one nierozerwalną częścią naszego życia – użytkownicy korzystają z nich w domu, na uczelni, na wakacjach, jak również w pracy (Pinola, 2011) (rysunek 2). Wszechobecność tych urządzeń i połączenie ich zastosowania jako telefonu prywatnego i firmowego może być źródłem pewnych problemów.

Rys. 2 Sposób wykorzystania smartfona (Źródło: Kaspersky Lab, 2011)

[57] Wydział Elektrotechniki, Automatyki i Informatyki, Politechnika Opolska

Korzystając ze smartfona do celów biznesowych, użytkownicy przechowują w jego pamięci cenne dla siebie kontakty (adresy e-mail, numery telefonów, dane poufne), notatki służbowe, łączą się z Internetem w celu przeprowadzania transakcji finansowych (rysunek 3). Ten sam smartfon może być również wykorzystywany do celów prywatnych, np. do przeglądania serwisów społecznościowych czy grania w mniej lub bardziej bezpieczne gry. Korzystanie z urządzenia mobilnego z bezprzewodowym Internetem, które cały czas znajduje się w ręce lub kieszeni użytkownika, sprawia, że użytkownik staje się mniej ostrożny i nie dba wystarczająco o bezpieczeństwo, tak jak w przypadku komputerów stacjonarnych czy laptopów (Asay, 2011). W efekcie smartfony zwierające coraz to więcej cennych informacji stają się okazją do nadużyć ze strony cyberprzestępców i stanowią potencjalne źródło ich dochodu (Niedzielewski, 2011a).

Pewność siebie, brak wyobraźni i niewiedza użytkowników smartfonów w kwestii dbania o ich bezpieczeństwo, są podstawowymi czynnikami zachęcającymi hakerów do przeprowadzania ataków i kradzieży cennych informacji. Główną przyczyną, kilkukrotnego wzrostu liczby zagrożeń i ataków na smartfony w ciągu ostatnich trzech lat, jest szereg zaniedbań ze strony producentów oprogramowania związanych z bezpieczeństwem telefonów komórkowych (Kowalski, 2011).



Rys. 3 Rodzaje przechowywanych danych w smartfonach (Źródło: Kaspersky Lab, 2011)

URZĄDZENIA MOBILNE W OGNIU ZAGROŻEŃ

Istnieje wiele zagrożeń i sposobów zainfekowania smartfona niebezpiecznym oprogramowaniem, które może wyrządzić na nim wiele szkód (Nachenberg, 2011). Pierwszym z nich są ataki powiązane z przeglądaniem stron internetowych. Są one zwykle inicjowane przez specjalnie do tego celu przygotowane strony internetowe lub przez dołączenie złośliwego kodu do

legalnie działających, zaufanych witryn. Po wejściu na taką stronę, wysyła ona do przeglądarki złośliwą treść, która następnie jest uruchamiana. Taki zabieg pozwala atakującemu na zainstalowanie złośliwego oprogramowania, kradzież poufnych danych czy też uszkodzenie zainstalowanego oprogramowania i danych znajdujących się w pamięci smartfona. Typowy atak oparty na sieci Web przebiega w następujący sposób: serwer, na którym umieszczona jest złośliwa strona, identyfikuje system operacyjny użytkownika wczytującego stronę jako potencjalnie zdatny do przeprowadzenia ataku. Zainfekowana strona wysyła specjalnie spreparowany zestaw danych do przeglądarki internetowej, powodując tym samym uruchomienie złośliwego kodu na urządzeniu użytkownika. Po przejęciu kontroli nad przeglądarką cyberprzestępca może otrzymać dostęp do historii przeglądarki internetowej, loginów i haseł, jak również może próbować wydobyć informacje z kalendarza czy bazy kontaktów.

Malware, czyli złośliwe oprogramowanie, jest kolejnym zagrożeniem dla bezpieczeństwa smartfonów. *Malware* może zostać podzielone na kilka kategorii: tradycyjne wirusy komputerowe, robaki komputerowe czy konie trojańskie. Tradycyjne wirusy komputerowe w wersji mobilnej są dołączane do legalnie dostępnych aplikacji dla smartfonów. Robaki komputerowe rozprzestrzeniają się w sieci pomiędzy urządzeniami. Konie trojańskie natomiast samodzielnie się nie rozprzestrzeniają. Zamiast tego wykonują szereg złośliwych działań, takich jak utrata poufności i integralności danych znajdujących się w smartfonie, wykorzystanie jego zasobów do złych celów lub nawet przejęcie kontroli nad urządzeniem i doprowadzenie do jego destrukcji.

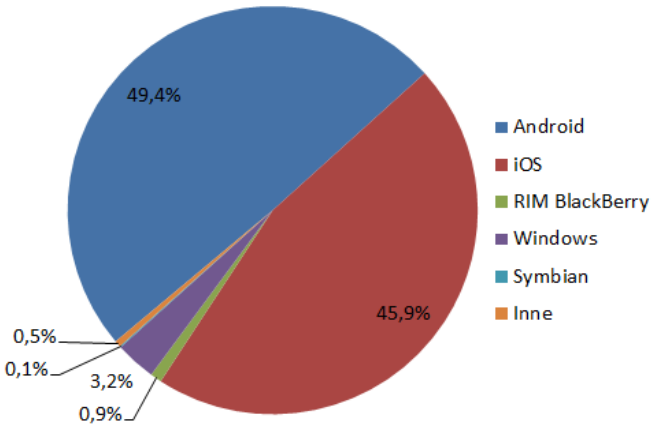
Kolejne zagrożenie jest związane z inżynierią społeczną (Goodchild, 2012). W kanonie bezpieczeństwa teleinformatycznego inżynierią społeczną nazywa się zbiór metod pozwalających na uzyskiwanie w sposób nielegalny niejawnych informacji przez cyberprzestępcę. Komputerowi oszuści wykorzystują niewiedzę i łatwowierność użytkowników systemów informatycznych na przykład do zainstalowania teoretycznie potrzebnego oprogramowania, które tak naprawdę jest oprogramowaniem szkodliwym. Popularną formą inżynierii społecznej jest tzw. phishing czyli wyłudzanie poufnych informacji od użytkowników poprzez podszywanie się pod instytucje. Przykładem może być wysyłanie wiadomości e-mail z prośbą o podanie haseł dostępu czy poprzez tworzenie fikcyjnych stron internetowych banków.

Równie istotnym i silnie rozwijanym zagrożeniem jest nadużywanie zasobów smartfonów przez osoby do tego niepowołane. Celem takich ataków jest spowolnienie działania nie tyle samych urządzeń, co całej sieci w której one pracują. Najpopularniejszą formą nadużywania zasobów jest tworzenie z urządzeń mobilnych tzw. „farm spamerskich", czyli źródła rozsyłania niechcianych wiadomości na inne urządzenia. Sytuacja przekazywania spamu jest inicjowana przez napastnika, który infekuje urządzenie ofiary. Ono zaś przejmuje rolę fabryki produkującej nowe wiadomości e-mail lub SMS będące spamem. Nieświadomy użytkownik staje się pośrednikiem w przekazywaniu wiadomości przesyłanych rzeszom niczego niespodziewających się kolejnych ofiar. W ten sposób źródłem spamu może stać się każde legalnie działające urządzenie. Innym przykładem jest wykorzystywanie zainfekowanych urządzeń do uruchamiania ataków DoS (ang. Denial of Service – odmowa usługi) wymierzonych na przykład przeciwko serwisom internetowym lub operatorom komórkowym. Atak DoS może przebiegać następująco: atakujący dokonuje wyboru urządzeń, które na przykład będą generowały ogromne liczby zapytań do serwerów www o dane lub usługi. Atak może mieć również formę ciągłego wysyłania wiadomości SMS z bardzo dużej liczby urządzeń.

Biorąc pod uwagę ograniczoną przepustowość sieci bezprzewodowych, takie ataki mogą potencjalnie wpłynąć na pogorszenie jakości zarówno usług głosowych, jak i transmisji danych.

FILARY BEZPIECZEŃSTWA MOBILNYCH SYSTEMÓW OPERACYJNYCH

Każde urządzenie mobilne jest wyposażone w system operacyjny, który zarządza procesami i usługami uruchamianymi na smartfonie. Obecnie na rynku smartfonów istnieje duża konkurencja, w której kluczową rolę odgrywają firma Google dostarczająca system Android na urządzenia m.in. Sony czy Samsunga, firma Apple z systemem operacyjnych iOS przeznaczonym na iPhony, firma BlackBerry z systemem operacyjnym BlackBerry OS oraz firma Microsoft z systemami Windows Mobile oraz Windows Phone 7 (rysunek 4).



Rys. 4. Popularność mobilnych systemów operacyjnych (Q4 2013 r.). Źródło: opracowanie własne na podstawie Koetsier (2013)

Projektanci architektury systemów operacyjnych iOS oraz Androida wprowadzili w różnym stopniu zaawansowania implementacje bezpieczeństwa. Można je podzielić na kilka odrębnych kategorii (Nachenberg, 2011). Pierwszą z nich jest tradycyjna kontrola dostępu. Polega ona na ochronie urządzenia przy użyciu zabezpieczeń takich jak hasło czy blokowanie ekranu urządzenia już nie tylko prostym gestem palca czy po upływie zadanego czasu bezczynności, lecz skomplikowanym wzorem kreślonym palcem po ekranie bądź kodem PIN wprowadzanym z poziomu klawiatury ekranowej. Kolejnym rozwiązaniem jest identyfikowanie pochodzenia aplikacji instalowanych na urządzeniu. Każda aplikacja powinna być opatrzona tożsamością autora, czyli jego podpisem cyfrowym. Daje to możliwość podjęcia przez użytkownika decyzji na temat chęci instalacji aplikacji danego autora lub niepodpisanej cyfrowo. W niektórych implementacjach wydawca oprogramowania może również analizować aplikację pod kątem odporności na zagrożenia przed jej opublikowaniem, dołączając do bezpiecznych aplikacji odpowiednie poświadczenia bezpieczeństwa. Istotnym rozwiązaniem jest szyfrowanie danych. Polega ono na ukryciu zawartości danego pliku znajdującego się na urządzeniu poprzez wykorzystanie do tego celu funkcji matematycznych. Ważnym rozwiązaniem jest też określenie uprawnień kontroli dostępu. Funkcjonalność taka określa uprawnienia zarówno aplikacji zainstalowanych w smartfonie, jak również możliwości ingerencji użytkownika w sam system operacyjny. Każda aplikacja ma przypisany zestaw uprawnień, który jest rygorystycznie kontrolowany w trakcie jej działania przez system operacyjny. Sprawdza on, czy określona aplikacja powinna mieć w danej chwili dostęp do

konkretnego podzespołu lub zbioru danych znajdujących się w pamięci. Aplikacje, które starają się przekroczyć swoje uprawnienia, powinny być blokowane przez jądro systemu. Ograniczenie uprawnień po stronie użytkownika ma na celu uniemożliwienie zaistnienia sytuacji, w której niedoświadczony użytkownik chciałby samodzielnie zaprogramować dodatkowe funkcje systemu. Źle skonfigurowany, modyfikowany system operacyjny może stanowić bardzo duże zagrożenie dla bezpieczeństwa. Dlatego użytkownik nie powinien posiadać uprawnień do zmiany niektórych opcji i parametrów systemu, które są krytyczne dla jego poprawnego funkcjonowania.

SYSTEM OPERACYJNY ANDROID FIRMY GOOGLE

Android firmy Google to darmowa platforma zawierająca zestaw oprogramowania przeznaczony na urządzenia mobilne – smartfony i tablety. Składa się ona z systemu operacyjnego, oprogramowania pośredniego, interfejsu użytkownika oraz dedykowanych aplikacji. Licencja Apache License czyni Androida popularnym, otwartym na rozwój ze strony użytkowników systemem. Platforma Android ma kilka kluczowych, charakterystycznych cech. Pierwszą z nich jest wirtualna maszyna Dalvik. Jest ona maszyną Java rozszerzoną o dostęp do wszystkich urządzeń telefonu, nie tylko klawiatury i głośnika. Takie rozwiązanie niesie ze sobą jednak pewne konsekwencje w kwestii bezpieczeństwa. Otóż, umożliwienie swobodnego dostępu apletom Dalvik do zasobów smartfona implikuje możliwość wykorzystania ich do celów niebezpiecznych dla smartfona i użytkownika. Szkodliwe oprogramowanie dołączone do zainstalowanej aplikacji może w ten sposób zaburzyć poprawne działanie systemu operacyjnego, spowodować kradzież cennych dla użytkownika danych lub nawet wysłać wiadomość SMS np. o podwyższonej płatności na specjalnie do tego celu przygotowany numer. Platforma Android teoretycznie jest zabezpieczona przed taką sytuacją. Ma ona bowiem zaimplementowany system kontroli uprawnień. Każda nowo uruchomiona aplikacja jest widoczna z poziomu menedżera procesów jako nowo powołany do życia proces. Użytkownik dzięki temu ma możliwość kontrolowania przydzielonych zasobów danej aplikacji oraz w przypadku podejrzenia jej nieprawidłowego działania zamknięcia danego procesu. Niestety, brak wiedzy o działaniu nowo pobranej aplikacji, może skutkować nieświadomym przydzieleniem krytycznych zasobów urządzenia destrukcyjnemu kodowi.

W ciągu ostatnich dwóch lat Android zdobył niekwestionowaną pozycję lidera wśród systemów operacyjnych oferowanych do smartfonów (Lech, 2011). To właśnie otwartość kodu i możliwość pisania własnych aplikacji oraz łatwość ich publikowania w Google Play (dawniej Android Market) przyczyniła się do ekspansji Androida.

Niestety, wraz z gwałtownym wzrostem popularności Androida, równie dynamicznie rośnie zainteresowanie cyberprzestępców tą platformą. Z miesiąca na miesiąc przybywa zagrożeń dla użytkowników tego systemu operacyjnego (Niedzielewski, 2011b; Wheatley, 2012). Głównym problemem firmy Google do końca 2011 roku była jej polityka bezpieczeństwa w kwestii przyjmowania nowych aplikacji do Google Play. W oficjalnym sklepie cyberprzestępcy mogli udostępniać aplikacje zawierające ukryty kod konia trojańskiego. Oczywiście zgłoszone przez użytkowników aplikacje co do których było podejrzenie, że ich działanie jest nieadekwatne do opisu, były sprawdzane i usuwane z Google Play. Na początku 2012 roku firma Google częściowo rozwiązała problem, wprowadzając usługę Bouncer. Jej zadaniem jest skanowanie aplikacji w poszukiwaniu znanego złośliwego kodu. Dodatkową funkcjonalnością tej usługi jest emulacja aplikacji, czyli próbne uruchomienie w odizolowanym środowisku. Niestety obie metody walki

z cyberprzestępcami mogą być w łatwy sposób ominięte. Jednym ze sposobów ominięcia usługi Bouncer (Freeman, 2012) jest włamanie się do konta znanego dewelopera, którego aplikacje nie są w niektórych przypadkach weryfikowane i z poziomu takiego konta udostępnienie szkodliwej aplikacji. W przypadku złamania zabezpieczenia w postaci emulacji aplikacji udostępnianych w Google Play, cyberprzestępca może zaprogramować szkodliwą aplikację w taki sposób, by w sytuacji wykrycia emulatora zmieniała charakter swojego działania i sprawiała wrażenie niegroźnej. Oczywiście, niezależnie od wprowadzenia przez Google usługi Bouncer, użytkownicy powinni nadal świadomie instalować aplikacje pobierane z poziomu Google Play.

Najnowsza wersja systemu operacyjnego Android, oznaczona jako 4.2.2, wprowadza szereg poprawek w kwestii bezpieczeństwa i uprawnień (Amadeo, 2013). Wśród głównych należy wymienić m.in. mechanizm Content Provider, który zarządza dostępem do ustrukturyzowanych kolekcji danych oraz uprawnieniami aplikacji i komponentów systemowych do wymiany tych danych (Chung, 2013). Poprzednie wersje systemu zezwalały na uzyskiwanie dostępu do danych aplikacji, które jednoznacznie nie miały zdefiniowanego zakazu ich odczytu. Winą za taki stan rzeczy można by również obarczać programistów, którzy jednoznacznie nie określali uprawnień aplikacji już na poziomie ich projektowania.

Rozprzestrzenianie się zagrożeń i infekowanie kolejnych urządzeń mobilnych jest spowodowane także w znacznym stopniu pobieraniem aplikacji mało znanych lub korzystanie z alternatywnych, nieoficjalnych Marketów. Instalując aplikację z innego źródła niż Google Play, należy liczyć się z dużym ryzykiem zainfekowania telefonu szkodliwym oprogramowaniem. Innym działaniem zagrażającym urządzeniom mobilnym jest instalowanie alternatywnych modyfikacji systemu operacyjnego Android oraz odblokowywanie zablokowanych w celach bezpieczeństwa przez Google niektórych funkcji systemu operacyjnego – tzw. *rooting* telefonu. Instalując alternatywne systemy operacyjne użytkownik musi się liczyć z faktem, że autor danej wersji mógł dodać do niego szkodliwe oprogramowanie, które na przykład wysyła wszystkie wykonane gesty i znaki wpisane z klawiatury. *Rooting* telefonu, który jest swego rodzaju bajpasem omijającym szereg zabezpieczeń systemu operacyjnego, ułatwia szkodliwym aplikacjom ingerencję w urządzenie. Nie muszą one już prosić o udostępnienie danego zasobu, tylko bez przeszkód same z niego korzystają.

Z chwilą wzrostu popularności oraz ekspansji systemu operacyjnego Android, z większą intensywnością pojawiały się coraz to bardziej niebezpieczne zagrożenia. Pierwszym odkrytym, wartym omówienia zagrożeniem był SMS Trojan (Irinco, 2010). Przedstawiony wirus instalował się na urządzeniu użytkownika jako znany z systemu operacyjnego Windows odtwarzacz plików multimedialnych – Windows Media Player. Aplikacja maskująca się pod ikonką wspomnianej aplikacji wysyłała wiadomości SMS na numery o podwyższonej płatności. Ta forma ataku była już wcześniej znana. Jej funkcjonalność została przeniesiona z platformy Symbian na nowy, zdobywający coraz większą popularność cel.

Najnowszymi zagrożeniami wycelowanymi w platformę Android była kolejna wersja SMS Trojana (Dr.WEB, 2012) oraz *malware* Loozfon i FinHisher, które zainteresowały przedstawicieli FBI (ang. Federal Bureau of Investigation) (Reyes, 2012), (Wheatley, 2012b). Wspomniany SMS Trojan został odkryty przez producenta oprogramowania antywirusowego – Dr.WEB. Aplikacja instalowała się na smartfonie pod nazwami App Store bądź Play Market i przyjmowała ikonki oficjalnego marketu z aplikacjami firmy Google – Google Play. Twórcy szkodnika zaimplementowali w nim dwie

funkcjonalności. Pierwszą z nich była możliwość wysyłania wiadomości SMS na numery o podwyższonej płatności. Druga funkcjonalność pozwalała dokonać transformacji smartfona w urządzenie będące źródłem ataków DoS w większej sieci przestępczej.

Zagrożeniami, które zostały zgłoszone przez FBI firmie Google, jako istotne do podjęcia działań zmierzających do zwiększenia bezpieczeństwa użytkowników, były *malware* Loozfon oraz FinFisher. Pierwszy szkodnik w głównej mierze potraktowany został jako koń trojański. Zainfekowane nim urządzenia mogły być sterowane przez ich autorów w celu uzyskania danych osobowych użytkownika. Drugi wspomniany *malware* – FinFisher – pozwalał cyberprzestępcom na zdalne monitorowanie miejsca pobytu urządzenia oraz przejmowanie nam nim kontroli.

Według raportu Mobile threat report Q4 2012 (F-Secure Labs, 2012), w ostatnim kwartale 2012 roku, zagrożenia wycelowane w system operacyjny Android stanowiły niemal 80% wszystkich ataków na mobilne systemy operacyjne. W porównaniu z analogicznym okresem roku poprzedniego, odsetek zagrożeń wycelowanych w system operacyjny Android wzrósł aż o 30 punktów procentowych. Co kwartał jest wykrywana nowa rodzina szkodliwego oprogramowania, która niesie za sobą różne warianty zagrożeń czyhających na cenne dane użytkowników smartfonów.

Nawet osoby instalujące tylko oficjalne wersje systemów operacyjnych oraz korzystające wyłącznie z oficjalnego sklepu Google Play są narażone na zagrożenia. Podobnie jak w przypadku systemów z rodziny Windows przeznaczonych na komputery, zaleca się korzystanie z oprogramowania antywirusowego. Wśród polecanych aplikacji wspomagających ochronę smartfona można wyróżnić m.in.: Lookout Security & Antivirus, avast! Mobile Security, Kaspersky Mobile Security, Norton Mobile Security Lite, NQ Mobile Security & Antivirus oraz ESET Mobile Security for Android. Wymienione aplikacje pochodzą od producentów znanych z programów antywirusowych na platformy rodziny Windows. Świadczy to o skali problemu jakim są zagrożenia dla bezpieczeństwa urządzeń mobilnych.

SYSTEM OPERACYJNY iOS FIRMY APPLE

Platformą konkurencyjną w stosunku do Androida jest iOS firmy Apple. Przeznaczony jest dla urządzeń mobilnych takich jak: iPhone, iPad oraz iPodTouch. Platforma iOS bazuje na systemie operacyjnym MAC OS X 10.5 firmy Apple oraz uniksowym jądrze Darwin. iOS jest hybrydą systemu operacyjnego Darwin, do którego dołączone zostało graficzne środowisko użytkownika Aqua. Podobnie, jak w przypadku systemu Android, iOS jest systemem udostępnianym na zasadach licencji Apple Public Source License, która pozwala uczestniczyć programistom w rozwijaniu produktów Apple.

System operacyjny iOS jest drugą platformą pod względem popularności wśród użytkowników urządzeń mobilnych. Przyjęty przez Apple model bezpieczeństwa dla iOS oferuje relatywnie silną ochronę przed złośliwym oprogramowaniem. Jest to efektem wprowadzonej polityki bezpieczeństwa, polegającej na intensywnym procesie weryfikacji aplikacji, które kandydują do udostępnienia w AppStore. Po pozytywnej weryfikacji, aplikacja jest podpisywana cyfrowym certyfikatem Apple. Dołączenie do elitarnego grona developerów aplikacji na iOS wiąże się również z koniecznością wniesienia rocznej opłaty za możliwość udostępniania aplikacji. Dla programistów indywidualnych jest to kwota 99$, natomiast dla firm 299$. Dodatkową innowacją wprowadzoną przez Apple jest iOS Developer Enterprise – program dedykowany firmom, dający możliwość

tworzenia izolowanych serwisów analogicznych do AppStore. Jest on dostępny jedynie dla zarejestrowanych urządzeń w danej firmie. Dodatkowo obok certyfikatów Apple, wystawiane są tu wewnętrzne certyfikaty firmy.

Taka polityka bezpieczeństwa pozwala eliminować ze społeczności programistów, tych udostępniających złośliwe aplikacje. Każde zarejestrowane konto może w każdej chwili zostać zablokowane w sytuacji wykrycia niepożądanego działania aplikacji napisanej przez posiadacza konta. Oczywiście, jak w przypadku Google Play, użytkownicy AppStore muszą liczyć się z możliwością wykradzenia im kont przez cyberprzestępców. System iOS charakteryzuje się również zamkniętością. Oznacza to, że użytkownik nie ma uprawnień administratora, co nie pozwala mu ingerować w system operacyjny. Ograniczenie to może zostać wyłączone poprzez uruchomienie procesu jailbreak (iDownloadBlog, 2011). Polega on na nieautoryzowanym przydzieleniu użytkownikowi praw administratora i daje możliwość instalowania aplikacji spoza AppStore.

ZASADY BEZPIECZEŃSTWA

Świadomość istniejących zagrożeń jest kluczem do uniknięcia konsekwencji z nimi związanych. Aby zmniejszyć ryzyko wyrządzenia szkód przez szkodliwe oprogramowanie na smartfonie należy przestrzegać kilku zasad (Internet Crime Complaint Center, 2012).

Kluczowym jest posiadanie zainstalowanego oprogramowania zabezpieczającego oraz regularne jego aktualizowanie. Równie istotnym jest regularne aktualizowanie zainstalowanych na smartfonie aplikacji, w celu posiadania najnowszych wersji. Takie postępowanie jest istotne w przypadku naprawienia przez producenta oprogramowania krytycznych luk związanych z bezpieczeństwem aplikacji. Pozwoli to uniknąć zainfekowania urządzenia użytkownika niepożądanym, złośliwym oprogramowaniem, które może wyrządzić na nim szkody w postaci utraty spójności danych bądź nawet ich usunięcia.

Ważne jest, tak jak w przypadku komputerów przenośnych, aby nie łączyć się z niezabezpieczonymi, bezprzewodowymi sieciami Wi-Fi. Sieci te mogą okazać się specjalnie przygotowanymi punktami dostępowymi, poprzez które cyberprzestępcy będę mogli infekować w prosty sposób. W przypadku przeglądania stron internetowych nie należy przechodzić na strony, których treści nie jesteśmy pewni. Podobnie należy postępować w kwestii pobierania plików i zapisywania ich w pamięci urządzenia mobilnego.

Przechowując dane poufne na urządzeniu, należy używać aplikacji umożliwiających ich szyfrowanie. Takie postępowanie uniemożliwi bądź w znacznym stopniu utrudni cyberprzestępcy ich odczytanie.

Wskazane jest wyłączanie lokalizacji GPS na urządzeniu. Nieustannie działający nadajnik GPS wskazujący lokalizację smartfona może zostać wykorzystany przez już nie tylko cyber- lecz realnych przestępców, którzy będą śledzili posiadacza zainfekowanego urządzenia.

Istotnym jest również zmiana domyślnych ustawień systemu operacyjnego w smartfonie. Część oprogramowania szkodliwego potrafi wyrządzić szkody jedynie na urządzeniach, które pracują właśnie na ustawieniach domyślnych.

W przypadku pobierania zaufanych aplikacji z oficjalnych źródeł bądź aplikacji o nieznanym pochodzeniu należy świadomie przechodzić kolejne etapy instalacji. Niewskazane jest przydzielanie instalowanym aplikacjom dostępu do krytycznych zasobów oraz funkcji systemu operacyjnego.

Instalując aplikację, która żąda udostępnienia krytycznego zasobu systemu operacyjnego, użytkownik powinien natychmiastowo przerwać instalację i zgłosić możliwe szkodliwe działanie aplikacji na portalu, z którego została pobrana. Przed pobraniem aplikacji użytkownik powinien przeczytać komentarze pozostałych internautów, którzy już wcześniej pobrali daną aplikację.

Zabronionym postępowaniem jest odblokowywanie zablokowanych w celach bezpieczeństwa krytycznych funkcji systemu operacyjnego. Procesy typu *jailbreak* oraz *rooting* umożliwiają dostosowywanie funkcjonalności oraz użyteczności smartfona do potrzeb jego użytkownika, lecz też otwierają drogę cyberprzestępcom do przejęcia nad nim kontroli. Każdorazowo, gdy dana aplikacja lub usługa systemowa jest uruchamiana w trybie nieograniczonym, umożliwia to przejęcie całkowitej kontroli nad nią lub nawet nad całym urządzeniem.

W przypadku chęci sprzedania urządzenia mobilnego, jego użytkownik powinien przywrócić wszystkie ustawienia domyślne systemu operacyjnego oraz smartfona. Zalecanym rozwiązaniem jest ponowna, czysta instalacja systemu operacyjnego. Pozwoli to uniknąć pozostawienia danych osobistych w pamięci urządzenia.

PODSUMOWANIE

Smartfony zastępują zwykłe telefony komórkowe. Przejmują dodatkowe funkcje domowych komputerów. Wykorzystywane są do sprawdzania poczty elektronicznej, edytowania dokumentów, przeglądania Internetu czy dokonywania transakcji bankowych.

Niezależnie od platformy, na której pracują użytkownicy oraz sposobu korzystania ze smartfona, powinni oni mieć świadomość istniejących zagrożeń. Warto przestrzegać podstawowych zasad zachowania się w Internecie (netykiety) oraz instalować w urządzeniu mobilnym dodatkowe oprogramowanie zabezpieczające. Należy instalować jedynie aplikacje pochodzące ze sprawdzonych, certyfikowanych źródeł, ponieważ zmniejsza to ryzyko zainfekowania smartfona złośliwym oprogramowaniem.

BIBLIOGRAFIA

Amadeo R. (2013) New Android 4.2.2 Features: Toggle From Quick Settings, Better App Download Notifications, and Some New Sounds!, dostęp 25 lutego 2013, http://www.androidpolice.com/2013/02/12/new-android-4-2-2-features-toggle-from-quick-settings-better-app-download-notifications-and-some-new-sounds/

Asay M. (2011) Safe as Windows: Smartphones' security nightmare, dostęp 5 stycznia 2013, http://www.theregister.co.uk/2011/10/28/smartphones_can_now_do_everything/

Cassavoy L. (2011) What Makes a Smartphone Smart?, dostęp 5 stycznia 2013, http://cellphones.about.com/od/smartphonebasics/a/what_is_smart.htm

Chung F. (2013) Security Enhancements in Jelly Bean, dostęp 25 lutego 2013, http://android-developers.blogspot.ro/2013/02/security-enhancements-in-jelly-bean.html

Dr.WEB (2012) New Trojan for Android can mount DDoS attacks, dostęp 25 lutego 2013, http://news.drweb.com/show/?i=3191

Freeman K. (2012) Google's Bouncer For Android Shows Malware Apps the Door, dostęp 5 stycznia 2013, http://mashable.com/2012/02/03/google-bouncer-for-android/

F-Secure Labs (2012) Mobile threat report Q4 2012, dostęp 25 lutego 2013, http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q4%202012.pdf

Goodchild J. (2012) Social Engineering: The Basics, dostęp 5 stycznia 2013, http://www.csoonline.com/article/514063/social-engineering-the-basics

iDownloadBlog (2011) How to Jailbreak the iPhone, iPad, iPod touch, and Apple TV, dostęp 5 stycznia 2013, http://www.idownloadblog.com/jailbreak/

Internet Crime Complaint Center (2012) Smartphone users should be aware of malware targeting mobile devices and safety measures to help avoid compromise, dostęp 25 lutego 2013, http://www.ic3.gov/media/2012/121012.aspx

Irinco B. (2010) First Android Trojan in the Wild, dostęp 25 lutego 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/first-android-trojan-in-the-wild/

Kaspersky Lab (2011) Badanie Kaspersky Lab: Korzystanie z Internetu mobilnego i świadomość związanych z nim zagrożeń wśród Europejczyków, dostęp 5 stycznia 2013, http://www.kaspersky.pl/about.html?s=news&newsid=1560

Koetsier J. (2013) Android's back, baby: Googles mobile operating system regains U.S. smartphone lead, dostęp 1 marca 2013, http://venturebeat.com/2013/02/25/androids-back-baby-edging-out-ios-for-u-s-smartphone-lead-with-cheap-phones/

Kowalski M. (2011) WYWIAD: Bezpieczeństwo urządzeń mobilnych, dostęp 5 stycznia 2013, http://pdaclub.pl/index.php?option=com_content&view=article&id=19521:wywiad-bezpieczestwo-urzdze-mobilnych&catid=36:firma/zastosowania&Itemid=104

Lech K. (2011) Android: zagrożenie ze strony malware rośnie w zatrważającym tempie, dostęp 5 stycznia 2013, http://www.pcworld.pl/news/377364/Android.zagrozenie.ze.strony.malware.rosnie.w.zatrwazajacym.tempie.html

Nachenberg C. (2011) Symantec Secutiry Response – A Window Into Mobile Device Secutrity, dostęp 5 stycznia 2013, http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

Niedzielewski D. (2011a) Android i bezpieczeństwo nie idą w parze, dostęp 5 stycznia 2013, http://www.networld.pl/news/372279_1/Android.i.bezpieczenstwo.nie.ida.w.parze.html

Niedzielewski D. (2011b) Smartfony podatne na ataki, dostęp 5 stycznia 2013, http://www.networld.pl/news/377674_2/Smartfony.podatne.na.ataki.html

Nielsen (2012) Smartphones Account for Half of all Mobile Phones, Dominate New Phone Purchases in the US, dostęp 5 stycznia 2013, http://www.nielsen.com/us/en/newswire/2012/smartphones-account-for-half-of-all-mobile-phones-dominate-new-phone-purchases-in-the-us.html

Pinola M. (2011) How to Choose the Best Smartphone for Work, dostęp 5 stycznia 2013, http://mobileoffice.about.com/od/phonesformobileworkers/a/selecting-a-smartphone-for-business.htm

Punzalan R. (2012) Smartphone Sales Projected to Grow Almost 40% This Year; dostęp 5 stycznia 2013, http://www.brighthand.com/default.asp?newsID=18981&news=smartphone+sales+projected+growth+2012

Reyes D. (2012) Android Malware Threats Issued By The FBI: Mobile Security You Need To Know, dostęp 25 lutego 2013, http://www.examiner.com/article/android-malware-threats-issued-by-the-fbi-mobile-security-you-need-to-know

Thomson I. (2013) Global smartphones sales set to outpace standard handsets in 2013, dostęp 5 marca 2013, http://www.theregister.co.uk/2013/03/04/smartphones_outsell_feature_phones_globally/

Wheatley M. (2012a) Chinese Android Malware Mayhem Goes Into Overdrive, dostęp 2 marca 2013, http://siliconangle.com/blog/2012/09/14/chinese-android-malware-mayhem-goes-into-overdrive/

Wheatley M. (2012b) FBI Warns OF Android Threats As Google Readies Malware Scanner, dostęp 25 lutego 2013, http://siliconangle.com/blog/2012/10/16/fbi-warns-of-android-threats-as-google-readies-malware-scanner/